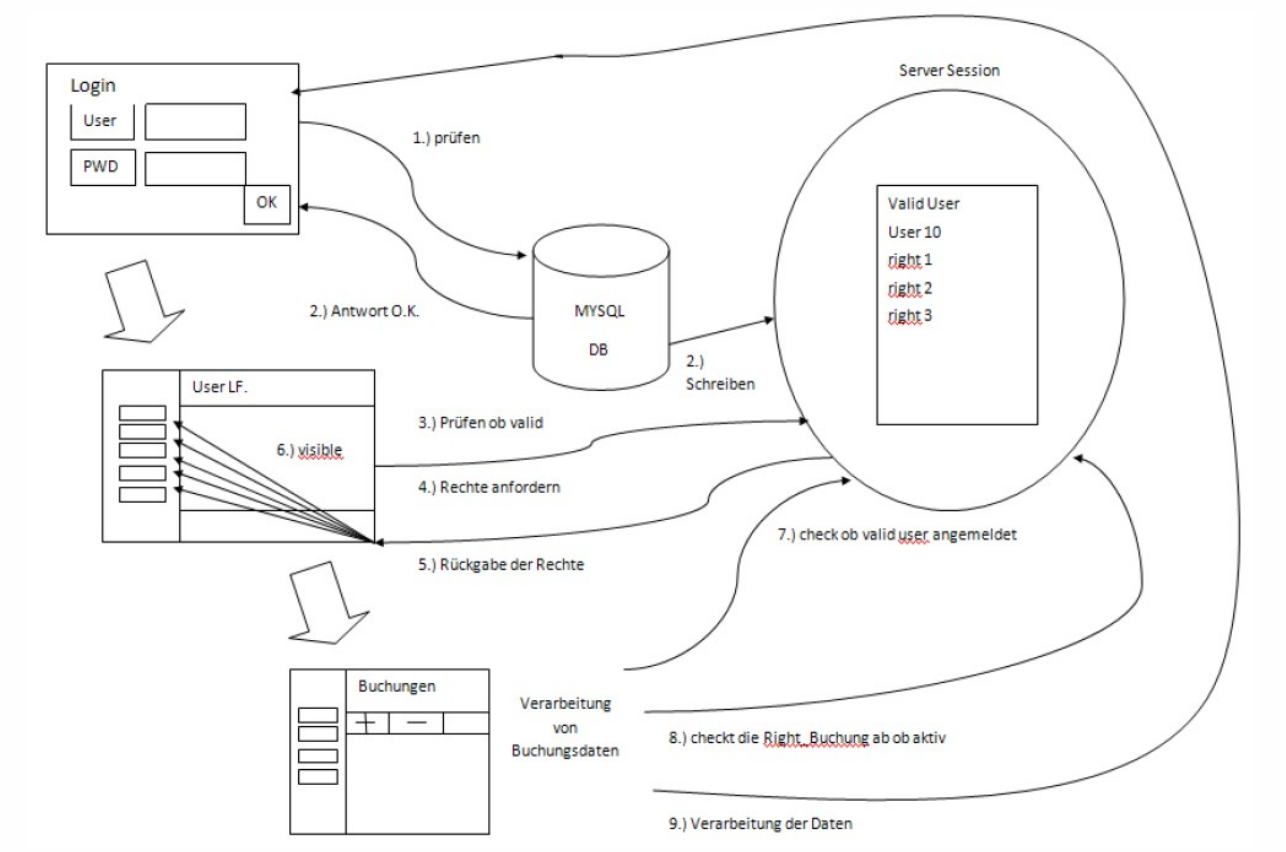
Security Konzept
Customer Processing

Schematische Darstellung:



Beim ersten Kontakt mit dem User wird ein Login-Fenster dargestellt und eine Benutzerauthentifizierung wird durchgeführt. Sobald der User seine Credentials eingegeben hat, werden das Passwort und die Mailadresse mit den gespeicherten Daten in der Datenbank kontrolliert. Das Passwort ist md5 codiert und wird erst am Server umgewandelt. Das bedeutet eine Übertragung des Passwortes vom Client zum Server in Klartext. Zur Lösung dieses Problems ist eine HTTPS-Verschlüsselung vorgesehen. Nachdem die Daten erfolgreich mit der Datenbank abgeglichen wurden, werden die entsprechenden Rechte des Users in die Serversession gespeichert. Danach wird der User zur eigentlichen Applikation weitergeleitet. Beim Aufbau der Applikation werden die Rechte, die in der Session gespeichert sind, abgefragt. Je nach Berechtigung werden die Navigationsbuttons auf „visible = true“ gesetzt und somit wird das Interface an die Berechtigungen des Users angepasst. Bei jedem weiteren Speichervorgang am Server, sowie beim Abrufen von Daten wird zuerst in der Session kontrolliert, ob ein valider User angemeldet ist. Danach wird geprüft, ob dieser User die entsprechenden Berechtigungen für die angeforderte Datenaktion besitzt. Falls das alles zutrifft, werden die Daten verarbeitet. Programmiertechnisch wurde die angestrebte Lösung durch definieren einer Klasse „SecurityObject“ erreicht, in dessen Constructor-Methode die Prüfung auf den angemeldeten User in der Session durchgeführt wird. Es existiert in dieser Klasse auch noch eine Methode, mit der ein Rechtevergleich durchgeführt werden kann.